DOI 10.36622/1682-7813.2024.27.1.006
УДК 004.056.57

СЕТЕВЫЕ АТАКИ С ПОМОЩЬЮ «СНИФФЕР-ПАКЕТОВ»: РАЗРАБОТКА ЧАСТНОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Золотарев, Д.А. Нархов, А.Н. Мокроусов, В.И. Борисов, А.Е. Дешина, А.С. Пахомова, А.Ю. Егоров

В статье рассматривается проблема разработки частных политик безопасности информации и регламентов обнаружения, реагирования и ликвидации последствий осуществления атаки с помощью «сниффер-пакетов», учитывающих особенности деятельности конкретных предприятий для более эффективной защиты от сетевых атак. Приводится частная политика информационной безопасности предприятия, разработанная на основе построенного риск-ландшафта для атак, проводимых с помощью «сниффер-пакетов».

Ключевые слова: корпоративная сеть, векторы атаки, уязвимости, риск-ландшафт, частная политика.

Введение

В настоящее время корпоративные сети повсеместно используются для обеспечения связи между компьютерами предприятий, которые могут находиться в одном здании либо располагаться на значительном удалении друг от друга. В связи с пандемией ковида стал набирать популярность удаленный формат работы, то есть получение сотрудниками доступа к корпоративной сети из дома, что породило новые риски для безопасности.

Опираясь на статистику, можно утверждать, что передача данных внутри сети не гарантирует полной безопасности в силу наличия уязвимостей программно-технических средств к различным способам перехвата сетевых пакетов. Хакеры активно используют методы сниффинга и перехватчики пакетов для кражи данных и конфиденциальной информации из электронной почты или веб-трафика по незащищенным сетям.

Поэтому защита корпоративных сетей от перехвата пакетов, в том числе с использованием нормативно-правового регулирования, выступает одним из ключевых аспектов обеспечения информационной безопасности [1-10].

Актуальность темы данного исследования обусловлена наличием противоречий между содержанием существующей нормативно-правовой базы регулирования информационной безопасности предприятий и потребностью практики в актуальных политиках, регламентах и инструкциях, учитывающих особенности атак с помощью «сниффер-пакетов».

Зачастую, атаки, проводимые с помощью «сниффер-пакетов», представляют довольно-таки серьёзную угрозу для корпоративной сети [1-10]. В частности, первичной целью злоумышленника является сбор информации о системе, что как раз и позволяет исследуемая атака. Основным последствием таких атак выступает нарушение конфиденциальности, однако, атаки, проводимые с помощью «сниффер-пакетов» оставляют серьезную брешь в системе защиты корпоративной сети. Ранее в ходе исследования был построен риск-ландшафт, что позволило определить наиболее опасные сочетания вектор атаки-уязвимость. Поскольку такие сочетания образуют множество сценариев, то сформированный перечень атак позволит грамотно выстроить систему защиты сети предприятия, и фундаментом для этого служит разработка частных политики и регламентов обеспечения информационной безопасности.

Разработка частных политики и регламентов обеспечения информационной безопасности предприятия

На сегодняшний день большинство крупных организаций разрабатывают собственные политики информационной безопасности (ИБ), опираясь на российские и международные стандарты такие как ГОСТ Р 50922-2006 Общие положения» [9], ISO/IEC 27001 [10], «Защита информации. Основные термины и определения», ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию и иные.

Небольшие организации зачастую берут за основу своей политики безопасности документы более крупных компаний, немного дорабатывают их и начинают применять на практике. Такой подход отличается неполнотой, наличием противоречий и направлен на защиту совершенно других компонентов.

Поэтому разработка регламентирующих документов организации в сфере ИБ должна базироваться на учете специфики актуальных сценариев атак, выделенных в процессе риск-анализа, и конкретных объектов защиты (активов). Объекты защиты организации от сетевой атаки с помощью «сниффер-пакетов» представлены в табл. 1. Частная политика защиты организации от сетевой атаки с помощью «сниффер-пакетов» включает систему взаимосвязанных мероприятий в ответ на последовательность действий злоумышленника в рамках реализации сценариев (табл. 2).

Таблица 1

Объекты защиты

Идентификатор объекта защиты	Сценарий атаки	Объект защиты
O_1	VA_1	АРМ пользователей
O_2	VA_2	Сетевые порты
O_3	VA_3	Сервер
O_4	VA_4	Операционная система
O_5	VA_5	Маршрутизатор

Таблица 2

Соответствие действий злоумышленника и мер противодействия им

Последовательность и содержание действий злоумышленника в целях реализации сценариев атаки типа «сниффер пакетов»	Меры защиты Организации от сетевой атаки типа «сниффер пакетов», адекватные действиям злоумышленника по каждому сценарию
1	2
Перечисление сетевых подключений (Network Connection Enumeration) VA_1	
1.1 Злоумышленник получает доступ к узлу сети жертвы.	1.1 Контроль выполняемых команд и аргументов, которые могут запрашивать подробную информацию о конфигурации сети и параметрах, таких как MAC и / или IP-адреса конечных точек, к которым они обращаются, или посредством удаленного обнаружения информации в системах. Отслеживание выполняемых команд и аргументов, с помощью которых возможно сформировать список подключений к скомпрометированной системе. Информация также может быть получена с помощью средств управления системой Windows, таких как инструментарий управления Windows и PowerShell.

Продолжение табл. 2

1	2
1.2 Злоумышленники могут выполнять перечисление сетевых подключений, чтобы обнаружить информацию о схемах связи устройств. Если злоумышленник может проверить состояние сетевого подключения с помощью таких инструментов, как Netstat, в сочетании с системным микропрограммным обеспечением, то он может определить роль определенных устройств в сети.	1.2 Мониторинг вызовов API (таких как GetAdaptersInfo() и GetIpNetTable()), которые могут собирать сведения о конфигурации сети и параметрах, таких как IP и / или MAC-адреса. Отслеживание вызовов API, позволяющих получить нарушителем список удаленных подключений к системе.
1.3 Злоумышленник также может использовать прослушивание сети для просмотра сетевого трафика на предмет получения подробной информации об источнике, пункте назначения, протоколе и контенте.	1.3 Отслеживание любых попыток включить скрипты, запущенные в системе, будет считаться подозрительным. Если скрипты обычно не используются в системе, но включены, подозрительными являются скрипты, выходящие из цикла из-за исправления или других функций администратора. Сценарии следует извлекать из файловой системы, когда это возможно, для определения их действий и намерений.
Прослушивание сети (Network Sniffing) VA_2	
2.1 Злоумышленник подключается к каналу передачи информации	2.1 Шифрование проводного и / или беспроводного трафика, когда это возможно и применение для веб-трафика, защищенного SSL / TLS.
2.2 Злоумышленник может попытаться прослушивать трафик, чтобы получить информацию о цели. Уровень важности этой информации может различаться. Относительно важной информацией могут быть данные для входа в систему	2.2 Ограничение доступа root или администратора к учетным записям пользователей, чтобы ограничить возможность захвата беспорядочного трафика в сети с помощью обычных инструментов захвата пакетов.
2.3 Учетные данные пользователя могут быть отправлены по незашифрованному протоколу, такому как Telnet, который может быть перехвачен и получен с помощью анализа сетевых пакетов.	2.3 Везде, где возможно, использование многофакторной аутентификации на основе современных протоколов (таких как Kerberos).
Удаленное обнаружение системы (Remote System Discovery) VA_3	
3.1 Злоумышленник подключается к сетевой инфраструктуре жертвы.	3.1 Отслеживание доступа к файлам (таким как /etc/hosts), позволяющих нарушителю сформировать список других систем по IP-адресу, имени хоста или иному логическому идентификатору в сети, который может использоваться для перемещения внутри системы.
3.2 Нарушитель может провести действия по получению списка других систем по IP-адресу, имени хоста или иному логическому идентификатору в сети.	3.2 Мониторинг аномалий, связанных с функциями ICS, связанными с обнаружением, включая устройства, которые ранее не использовали эти функции, или для функций, отправляемых на множество внешних станций. Внимание к некоторым протоколам ICS, использующим широковещательную или многоадресную рассылку, что может приводить к ложным срабатываниям.

Окончание табл. 2

1	2
3.3 Полученная информация может быть использована для последующего перемещения внутри системы. В этом случае в качестве инструментов злоумышленников могут выступать функциональные возможности и утилиты, доступные в операционной системе или программном обеспечении поставщика.	3.3 Мониторинг новых выполняемых процессов, которые могут быть использованы для обнаружения удаленных систем, таких как ping.exe и tracert.exe, особенно при выполнении в быстрой последовательности.
Удаленное обнаружение системной информации (Remote System Information Discovery) VA_4	
4.1 Злоумышленник подключается к основным концентрирующим сетевым устройствам (FTP сервер).	4.1 Физическое ограничение доступа к сетевым портам и отключение не используемых портов. Настройка межсетевых экранов на доверенный входящий и исходящий трафик внутри сети.
4.2 Злоумышленник может попытаться получить подробную информацию об удаленных системах и их периферийных устройствах, таких как марка / модель, роль и конфигурация	4.2 Сегментация структуры корпоративной сети таким образом, чтобы злоумышленнику было недостаточно доступа к одной сетевой машине для захвата нужной информации.
4.3 Злоумышленники могут использовать информацию, полученную при удаленном обнаружении системной информации, для помощи в нацеливании и формировании последующего поведения. Кроме того, конфигурация системы может быть использована для определения области последующего применения технологии[3].	4.3 Своевременное изменение системной информации корпоративной сети и службы передачи данных.
Беспроводное прослушивание (Wireless Sniffing) VA_5	
5.1 Злоумышленник находится в зоне действия беспроводной сети или получил доступ к маршрутизатору.	5.1 Ограничение доступа к сети (Подключение только доверенным Ip и Mac адресам) и ограничение радиуса действия беспроводного сигнала, в том числе методом экранирования сигнала.
5.2 Злоумышленник подключается к нешифрованной Wi-Fi сети.	5.2 Шифрование всего внутреннего и внешнего трафика беспроводной сети (SSL/TLS и VPN).
5.3 Злоумышленник использует сниффер для перехвата трафика между устройствами, подключенными к сети, и собирает конфиденциальную информацию.	5.3 Использование сетевого брандмауэра для блокировки подозрительного трафика.

На основе мер частной политики (табл. 2) возможно предложить мероприятия и средства для включения в регламенты обнаружения (табл. 3), реагирования (табл. 4) и устранения последствий инцидентов (табл. 5).

Таблица 3

Обнаружение и регистрация инцидентов безопасности

Типы инцидентов, которые могут возникнуть при реализации действий злоумышленника в ходе сетевой атаки типа «сниффер пакетов»	Описание инцидента	Средства для обнаружения заданного типа инцидента
Перечисление сетевых подключений (*Network Connection Ennumeration*) VA_1		
Компрометация учетных записей	Инцидент связан с неправильной аутентификацией пользователей	1.Управление учетными данными в СЗИ 2.Использование многофакторной аутентификации пользователей
Прослушивание сети VA_2		
Контроль доступа конфиденциальности, целостности данных	Инцидент связан с неправильной передачей конфиденциальной информации	1.Использование лицензированного антивирусного ПО 2.Анализ трафика корпоративной сети 3.Системы предотвращения утечек данных
Удаленное обнаружение системы (Remote System Discovery) VA_3		
Сбор информации об инфраструктуре системы и системных данных	Инцидент связан с мошенничеством с использованием ИКТ	1.Использование средств контроля от НСД 2.Системы обнаружения вторжений (IDS) 3.Межсетевые экраны
Удаленное обнаружение системной информации (Remote System Information Discovery) VA_4		
Получение доступа к системным данным организации	Инцидент, связан с несанкционированным доступом и компрометацией информации	1.Использование СКЗИ 2.Анализ событий безопасности 3.Межсетевые экраны
Беспроводное прослушивание (Wireless Sniffing) VA_5		
Несанкционированный доступ к каналу передачи данных	Инцидент связан с несанкционированным доступом и компрометацией информации	1.Сканеры уязвимостей и средства аудита 2.Антивирусное ПО 3.Системы предотвращения утечек данных

Таблица 4

Реагирование на инциденты безопасности

Произошедшие инциденты в ходе действий злоумышленника в целях реализации сценариев атаки типа «сниффер пакетов»	Первоочередные меры по предотвращению инцидента	Негативные последствия, вызванные инцидентом безопасности
1	2	3
Перечисление сетевых подключений (Network Connection Enumeration) VA_1		
Компрометация учетных записей	1.Удаление учетных данных из реестра 2.Проверка работоспособности шифрования трафика аутентификации 3.Проверка протоколов аутентификации	1.Раскрытие конфиденциальной информации 2.Несанкционированный доступ

Продолжение табл. 4

1	2	3
Прослушивание сети (Network Sniffing) VA_2		
Контроль доступа конфиденциальности, целостности данных	1. Блокировка всего входящего/исходящего трафика 2. Блокировка всех процессов аутентификации/верификации 3.Резервное копирование данных	1.Нарушение доступа к информации 2.Нарушение конфиденциальности информации 3.Потеря целостности информации
Удаленное обнаружение системы (Remote System Discovery) VA_3		
Сбор информации об инфраструктуре системы и системных данных	1.Отключение сегмента узла корпоративной сети 2.Остановка протоколов маршрутизации	1.Раскрытие инфраструктуры сети 2.Утечка системной информации сети
Удаленное обнаружение системной информации (Remote System Information Discovery) VA_4		
Получение доступа к системным данным организации	1. Отключение всех неиспользуемых служб 2. Ограничение доступа к объекту атаки в сегменте сети	1.Индикаторы возможных проблем в программных средствах защиты информации, такие как сбои, перезагрузки 2. Изменение параметров маршрутизации
Беспроводное прослушивание (Wireless Sniffing) VA_5		
Несанкционированный доступ к каналу передачи данных	1. Анализ трафика 2. Завершение всех неопознанных активных сеансов	1.Нарушения функционирования сетевых служб 2. Неправильная работа аутентификации 3. Некорректная работа прав доступа в СЗИ

Таблица 5

Ликвидация последствий инцидента безопасности

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
Перечисление сетевых подключений (Network Connection Ennumeration) VA_1	
1.Раскрытие конфиденциальной информации 2.Несанкционированный доступ	1.Использование защищенных методов аутентификации пользователей 2.Использование актуальных протоколов шифрования передачи данных 3.Изменение актуальных данных авторизации пользователей
Прослушивание сети (Network Sniffihg) VA_2	
1.Нарушение доступа к информации 2.Нарушение конфиденциальности информации 3.Потеря целостности информации	1. Восстановление данных, если они были утрачены или скомпрометированы в результате инцидента 2. Изменение всех данных учетных записей для потери актуальности украденной информации
Удаленное обнаружение системы (Remote System Discovery) VA_3	
1.Раскрытие инфраструктуры сети 2.Утечка системной информации сети	1.Выполнить сегментацию сетевой инфраструктуры предприятия 2.Удалить все системные записи 3.Отключение системных протоколов передачи информации
Удаленное обнаружение системной информации (Remote System Information Discovery) VA_4	
1.Индикаторы возможных проблем в программных средствах защиты информации, такие как сбои, перезагрузки и лишний трафик 2. Изменение параметров маршрутизации	1. Изоляция компрометированной системы или сети от остальной части инфраструктуры, чтобы предотвратить распространение или доступ злоумышленников к другим системам 2. Остановка всех процессов, связанных с инцидентом, например, удаление или блокировка учетных записей злоумышленников 3.Возвращение настроек и параметров маршрутизации, если они были изменены или нарушены

Окончание табл. 5

1	2
Беспроводное прослушивание (Wireless Sniffing) VA_5	
1.Нарушения функционирования сетевых служб 2. Неправильная работа аутентификации 3. Некорректная работа прав доступа в СЗИ	1. Перезапуск систем анализа трафика 2. Проверка работы защиты, шифрования и обнаружения инцидентов 2. Восстановление настроек сети, прав доступа, если произошел сбой 3. Поиск активных снифферов с помощью анализа трафика

Обучение сотрудников базовым мерам по защите информации, что не только повышает квалификацию самих сотрудников, но и способствует снижению рисков.

Выработанные меры по защите информации позволят значительно снизить риск реализации векторов атак, приведенных в табл. 1.

Заключение

Таким образом, атаки с помощью «сниффер-пакетов» на сегодняшний день не утратили актуальности, несмотря на развитие технологий шифрования и защиты от прослушивания трафика. Данный вид атак часто используется как этап для получения НСД к корпоративным сетям другими способами. Для минимизации рисков, связанных с атаками, проводимых с помощью «сниффер-пакетов», следует не ограничиваться только программно-аппаратными средствами защиты, но также уделять время и усилия, чтобы сотрудники предприятий соблюдали правила использования и передачи конфиденциальной информации.

Для повышения эффективности защиты корпоративной сети организации от атак, проводимых с помощью «сниффер-пакетов» предлагается:

− разработка собственных систем защиты, соответствующих российским и международным стандартам;

− внедрение средств шифрования и туннелирования каналов передачи информации;

− использование в рамках корпоративной сети актуального ПО;

− контроль и анализ всего передаваемого трафика внутри корпоративной сети;

− разработка частной политики безопасности с учетом специфики организации и особенностей атаки;

− проведение регулярных исследований в области защиты информации;

− проведение обучения пользователей мерам соблюдения информационной безопасности в условиях атак.

Соблюдение перечисленных мер должно существенно сократить риск успешных атак, проводимых с использованием «сниффер-пакетов» и повысить безопасность корпоративной сетей, в том числе на объектах критической инфраструктуры.

Список литературы

1. База знаний MITRE. URL: https://attack.mitre.org/ (дата обращения 29.01.24).

2. Common Attack Pattern Enumeration and Classification.URL: https://capec.mitre.org (дата обращения 29.01.24).

3. DataSet UNSW-NB15. URL: https://www.kaggle.com/datasets/alextamboli/unsw-nb15 (дата обращения 29.01.24).

4. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения 29.01.24).

5. Перечисление общих недостатков.URL: https://cwe.mitre.org/index.html (дата обращения 29.01.24).

6. Национальная база данных уязвимостей. URL: https://nvd.nist.gov/ (дата обращения 29.01.24).

7. Уязвимости и угрозы сниффер-пакетов в 2020-2021 гг. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/ (дата обращения 29.01.24).

8. GitHub База данных машинного обучения алгоритмам обнаружения сетевых атак. URL: https://github.com/srtk88/Machine-

learning-algorithms-for-detecting-network-attacks-with-UNSW-NB15-data-set (дата обращения 29.01.24).

9. Стандарты в области информационной безопасности. URL: https://www.altell.ru/legislation/standards/ (дата обращения 29.01.24).

10. ISO/IEC 27001. Системы менеджмента информационной безопасности.URL: https://www.iso.org/ru/standard/27001 (дата обращения 29.01.24).

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 03.02.2024

Информация об авторах

Золотарев Алексей Александрович – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Мокроусов Александр Николаевич – старший преподаватель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Борисов Василий Иванович – д-р техн. наук, профессор, профессор, Воронежский государственный технический университет, e-mail: lexanderostapenkoias@gmail.com

Дешина Анна Евгеньевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Пахомова Анна Степановна – канд. техн. наук, с.н.с., доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Егоров Анатолий Юрьевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS USING "SNIFFER PACKETS": EVELOPMENT OF A PRIVATE INFORMATION SECURITY POLICY

A.A. Zolotarev, D.A. Narkhov, A.N. Mokrousov, V.I. Borisov, A.E. Deshina, A.S. Pakhomova, A.Y. Egorov

The article discusses the problem of network attacks using "sniffer packets" and substantiates the relevance of this problem. Attention is focused on the importance of developing private information security policies that take into account the specifics of the activities of specific enterprises for more effective protection against network attacks using "sniffer packets". A private information security policy of the enterprise is presented, developed on the basis of a built risk landscape for attacks carried out using "sniffer packets".

Keywords: corporate network, attack vectors, vulnerabilities, risk landscape, private policy.

Submitted 03.02.2024

Information about the authors

Alexey A. Zolotarev – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Dmitry A. Narhov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander N. Mokrousov – Senior Lecturer, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Vasily I. Borisov – Doctor of Technical SciencesPhD, Professor, Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Anna E. Deshina – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Anna S. Pakhomova – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Anatoly Y. Egorov – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com